REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant advises that a change of correspondence address is being filed with this response. Applicant also advises that the attorney docket number for the present application has changed, and the new attorney docket number is noted above. Applicant kindly requests that the Office amend its records to indicate same.

Amendments to the Claims

Claims 1, 9 and 10 are amended to specify the physical use of the computed point multiple, key and elliptic curve digital signature respectively, computed therein, namely for cryptographic operations in cryptographic systems. Various other typographic errors are also amended. No new subject matter is believed to be added by way of these amendments.

Claim 10 is also amended replacing "said endomorphism" with "an endomorphism" to thereby refer to an indefinite article.

Claim 8 is amended to include a definition for the variable "m", namely that it is the extension degree of a finite field over which the elliptic curve is defined. Support for this amendment can be found in paragraph [0005] of the application as published, wherein the finite field F_{2^m} is introduced. Accordingly, no new subject matter is believed to be introduced by way of this amendment.

Claim Rejections – 35 U.S.C. §112, second paragraph

Claim 8 was rejected under 35 U.S.C. §112, second paragraph for insufficient antecedent basis for the variable "m". Claim 8 is amended as described above, and is believed to comply with 35 U.S.C. §112, second paragraph.

Claim 10 was rejected under 35 U.S.C. §112, second paragraph for insufficient antecedent basis for the limitation "said endomorphism". Claim 10 is amended as described above, and is believed to comply with 35 U.S.C. §112, second paragraph.

Claim Rejections - 35 U.S.C. §101

Claims 1-12 were rejected under 35 U.S.C. §101 for being directed to non-statutory subject matter. Claims 1, 9 and 10 are amended as indicated above to specify the physical use of the computed point multiple (claim 1), key (claim 9), and elliptic curve digital signature (claim 10), computed therein, namely for cryptographic operations in cryptographic systems. Claims 2-8 and 11-12 are either directly or indirectly dependent on claims 1 and 10 respectively, and further define certain limitations of the respective parent claim.

Applicant refers to *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F.3d 1368 (Fed. Cir. Jul. 23, 1998) (hereinafter "*State Street*"). In *State Street*, the question of statutory subject matter under 35 U.S.C. §101 was a primary issue. Section 101 reads: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."

In *State Street*, two exceptions to statutory subject matter were discussed, one being the "mathematical algorithm" exception, which is most relevant to the subject matter of the present application. The Supreme Court has identified three categories of subject matter that are unpatentable, namely "laws of nature, natural phenomena, and abstract ideas." [*Diamond v. Diehr*, 450 U.S. 175 (1981)]. Of particular relevance to the *State Street* case, the Court has held that mathematical algorithms are not patentable subject matter to the extent that they are merely abstract ideas. Moreover, in *Diamond v. Diehr*, the Court explained that certain types of mathematical subject matter, standing alone, represent nothing more than abstract ideas until reduced to some type of practical application, i.e., "a useful, concrete and tangible result."

Unpatentable mathematical algorithms are identifiable by showing they are merely abstract ideas constituting disembodied concepts or truths that are not "useful." However, from a practical standpoint, this means that to be patentable an algorithm must be applied in a "useful" way. For example, the court has held that data transformed by a machine through a series of mathematical calculations to produce a smooth waveform display on a rasterizer monitor, constituted a practical application of an abstract idea (a mathematical algorithm, formula, or

calculation), because it produced "a useful, concrete and tangible result" - the smooth waveform. [*In re Alappat*, 33 F.3d 1526, 1540-41, 31 USPQ2d 1545, 1554 (Fed. Cir. 1994)]

Similarly, in *Arrythmia Research Technology Inc. v. Corazonix Corp.* , 958 F.2d 1053, 22 USPQ2d 1033 (Fed. Cir. 1992), the Court held that the transformation of electrocardiograph signals from a patient's heartbeat by a machine through a series of mathematical calculations constituted a practical application of an abstract idea (a mathematical algorithm, formula, or calculation), because it corresponded to a useful, concrete or tangible thing-the condition of a patient's heart.

Turning again to *State Street*, the Court held that the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces "a useful, concrete and tangible result"-a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades.

In the present application, the claims are directed towards the computation of point multiples in an elliptic curve cryptosystem, for performing cryptographic operations. By performing the steps set out in claims 1, 9 and 10, a useful concrete and tangible result is obtained, namely a value corresponding to a multiple of a point on an elliptic curve. This is a concrete and tangible value. It is useful as recited in the claims in cryptographic operations where multiples of a point are required in generation of keys, performing signature and verification, for example. It is well known that cryptographic operations involve the practical application of mathematics to generate, e.g., cryptographic keys for use in cryptographic systems. To perform these functions it is necessary to obtain and use a value that is a multiple of a point. Doing this efficiently and securely is of paramount importance. The decision set forth in *State Street* is therefore believed to be relevant to the issue at hand, and the logic used in *State Street* should apply. Accordingly, Applicant believes the claims of the present application involve the practical application of mathematical formulas to produce tangible results, namely the point multiple of claim 1, the key of claim 9, and the elliptic curve digital signature of claim 10.

Accordingly, Applicant believes that the amended claims 1-12 submitted herewith constitute statutory subject matter. Therefore, claims 1-12 are believed to comply with 35 U.S.C. §101.

Claim Rejections – 35 U.S.C. §102(e)

Claims 1-12 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,430,588 to Kobayashi et al. Applicant respectfully traverses the rejections as follows.

The present application generally describes and claims a method for providing a point multiple in an elliptic curve cryptosystem to be used for performing cryptographic operations (claim 1). Several embodiments exemplifying uses of such a method are also described and claimed, in particular, for computing a key (claim 9) and an elliptic curve digital signature (claim 10).

The methods claimed in the present application, in part, recite a step of "computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve". The pair of coefficients are previously derived from a truncator of the elliptic curve. The point multiple is computed using the computed representation of the scalar and a Frobenius mapping τ. Each of claims 1, 9 and 10 recite such steps.

Kobayashi teaches a method for performing elliptic curve arithmetic for m-multiplying a rational point P over an elliptic curve $\frac{E}{GF(q)}$ defined over a finite field. The Examiner relies primarily on a passage in column 3, lines 25-52 of Kobayashi. In this passage, Kobayashi generally describes a method consisting of taking a rational point P, a Frobenius map ϕ, an integer k, a prime q; calculating integers r and c_i using the Frobenius map; calculating r points (P_0, P_1, ..., P_{r-1}); calculating mP using P, r and c_i using table reference addition while being supplied with the points P_0, ..., P_{r-1}; and outputting the calculated mP.

Kobayashi does not perform the step of computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve. Moreover, Kobayashi does not derive a pair of coefficients from a truncator of the elliptic curve nor compute a point multiple based on the representation and a Frobenius mapping. In fact, Kobayashi computes the integers r and c_i using a Frobenius map, and calculates the point mP using table reference. This is quite different from what is recited in claims 1, 9 and 10. Most

notably, in Kobayashi, the integers are computed using a Frobenius map, and the point mP is computed using table reference, whereas claims 1, 9 and 10 derive coefficients from a truncator and derive the point multiple, in part, from the Frobenius mapping. Clearly Kobayashi teaches an entirely different method than what is recited in claims 1, 9 and 10.

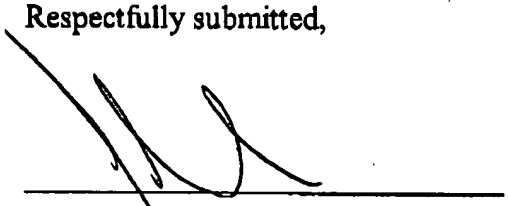
Accordingly, Kobayashi does not teach every element of any of claims 1, 9 and 10. Therefore Kobayashi cannot anticipate claims 1, 9 and 10; and claims 1, 9 and 10 are believed to clearly and patentably distinguish thereover. Claims 2-8 and 11-12 in their dependencies on claims 1 and 10 respectively are also believed to distinguish over Kobayashi.

Summary

In view of the foregoing, Applicant believes that amended claims 1-12 submitted in this response constitute statutory subject matter, and clearly and patentably distinguish over the prior art cited by the Examiner.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: September 22, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL